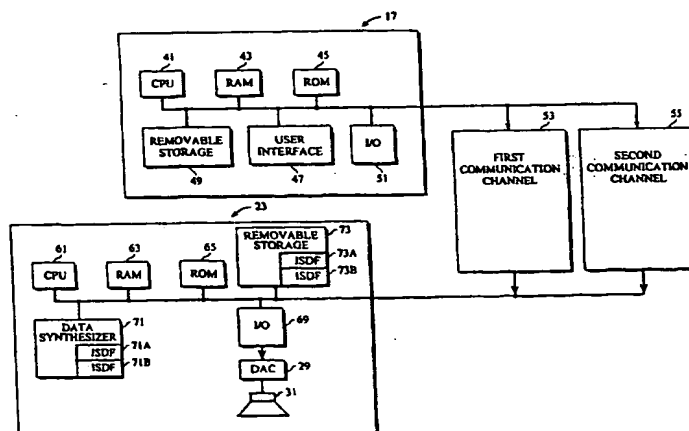




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G10H 1/00, H04L 9/00		A1	(11) International Publication Number: WO 00/49597
			(43) International Publication Date: 24 August 2000 (24.08.00)
(21) International Application Number: PCT/US00/04012		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 16 February 2000 (16.02.00)			
(30) Priority Data: 60/120,717 16 February 1999 (16.02.99) US			
(71) Applicant (for all designated States except US): TUNETO.COM, INC. [US/US]; 303 Twin Dolphin Drive, Redwood City, CA 94065 (US).			
(72) Inventor; and (75) Inventor/Applicant (for US only): BRATTON, Timothy [US/US]; 101 First Street, PMB 549, Los Altos, CA 94022 (US).			
(74) Agents: SCHIPPER, John et al.; Sabath & Truong, Suite 815, 111 North Market Street, San Jose, CA 95113 (US).		Published With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.	

(54) Title: AUDIO SYNTHESIS USING DIGITAL SAMPLING OF CODED WAVEFORMS



(57) Abstract

Method and system for audio synthesis of a digital data file representing an assembly of information-bearing sounds (15) in digital form. One or more spaced apart data segments are designated as key blocks (19) and are removed from the original data file. The remainder (21) of the data file is encrypted or otherwise encoded and communicated to a selected recipient on a first channel (53). Locations, sizes and separation distances of key blocks from each other within the original data file and a selected portion of the encoding or encryption key are placed in a data supplement. The removed segments and data supplement (optional) are communicated to the selected recipient on a second channel (55) and/or at another time. The original data file is recovered by using the data supplement information, or using already available information, decoding or decrypting the encoded or encrypted data file and replacing the removed segments within the data file remainder. Neither the remainder data file nor the removed segments plus data supplement is sufficient, by itself, to allow reproduction of the original data file. Each of the remainder data file and the removed segments plus data supplement can be distributed separately and subsequently combined when authorization or license to reproduce the sounds has been obtained.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CJ	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

AUDIO SYNTHESIS USING DIGITAL SAMPLING OF CODED WAVEFORMS

Field of the Invention

5 This invention relates to coding and reproduction of audio signals.

Background of the Invention

Digital synthesizers or other electronic systems that create music or other sound can often be utilized as an electronic musical instrument or electronic sound machine. A digital synthesizer is often arranged to accept
10 signals from a musician or operator interface and to produce digital output signals that represent analog signals in the audio frequency range. A digital synthesizer is also frequently arranged to accept pre-recorded sequences of music events in a Musical Instrument Digital Interface (MIDI) format.

A digital output signal from a digital synthesizer can be converted to
15 an analog signal and delivered to equipment, such as a loudspeaker, tape recorder, mixer or other similar device, to reproduce the signals as intelligible sound. The digital synthesizer can be arranged to provide output signals that simulate the sounds of one or more conventional musical instruments. Alternatively, the synthesizer can be arranged to simulate
20 sounds that would be emitted by a theoretical instrument having predetermined audio characteristics that are partly or wholly different from the corresponding characteristics of any convention, known instrument.

For previous synthesizers, synthesis of music and other sounds is a formidable task. A real musical instrument produces a complex blend of
25 many different frequencies and impart what is commonly referred to as "tone color" or "timbre" to the associated sound. For example, a percussion sound made by a drum or cymbal is an aperiodic sound that cannot be fully described by any simple mathematical function. Accordingly, the

reproduction or synthesis of digital signals representing sounds as rich and complex as a real musical instrument is a formidable task for digital signal sampling and processing. Ideally, the synthesizer should respond to the nuances of a musician's manipulation of the interface (e.g., a particular musical instrument). For example, a snare drum has many different audio characteristics when played in different locations, such as adjacent to the center of the drum membrane, adjacent to the rim, or on the rim of the drum. Additionally, the audio characteristics of a percussion instrument will vary with the striking force and stylistic inflection of the musician.

By providing a large enough waveform database, more realistic and expressive synthesis of a given group of sounds can be achieved. Many synthesizers relying on waveform sampling technology are used extensively in the music and multimedia fields for their ability to create musical sounds that closely emulate the sound of a musical instrument.

At present, a digital synthesizer system often utilizes a MIDI to control the synthesizer. The MIDI interface creates control signals or other MIDI control data. The MIDI control data may represent a music event, such as occurrence of specific musical notes from a particular musical instrument, such as a piano, drum or horn. However, MIDI has some fundamental limitations. For example, a synthesizer that uses a MIDI notation has trouble recreating a human voice.

A conventional synthesizer system utilizes a large solid state memory that stores the digital waveform signals representing each note played on a particular instrument. The memory can be a static random access memory (SRAM), a dynamic random access memory (DRAM), a read only memory (ROM) or some other similar memory with sufficiently rapid response.

When a musician actuates a key or other interface device, the appropriate waveform is selected, depending upon the key actuated and upon the

intensity and velocity of the key strike. The waveform is then converted into an analog output signal for sound reproduction. A digital waveform signal can be combined with other waveform signals that represent other musical notes being displayed, before the conversion to an analog output signal.

5 In this arrangement, the synthesizer, in effect, merely plays back digital recordings of individual musical notes or other sounds. Each waveform signal is stored as a collection of individual data words, each representing a single sample of the waveform at a particular time.

A sequencer is a device for editing musical data, such as MIDI events, and converting the musical data into a musical signal in real time. 10 Synthesizers are frequently used together with a computer to play a musical score. In this arrangement, a sequencer reads a MIDI file as an ordered sequence. However, it is generally recognized that MIDI files and synthesizers are unable to recreate the nuances in a recording or to capture 15 the background noises of a live audience.

Other prior art systems store only one or a relatively few waveform signals representing each musical instrument. These stored waveforms are then adjusted by digital signal processing or other electronic techniques, such as nonlinear distortion, to reflect the frequency and amplitude changes 20 associated with particular musical characteristics, as indicated by the MIDI control data. For example, the frequency and amplitude of a sample waveform representing middle C on a piano can be adjusted to synthesize a different piano note and volume. However, these synthesizers are unable to (re)produce the complex blends or tone color with high enough fidelity for 25 the musically trained ear.

In another approach, some systems use digital filtering to adjust the harmonic content of a particular note. However, these systems require a

large amount of computer power and can be affected by audio quality degradation.

What is needed is an audio synthesizer system that can reliably reproduce all types of sounds, including music and the human voice.

- 5 Preferably, the system should allow a separation of music or other information-bearing sound into two or more selected components, where no single component allows reproduction of sounds resembling the original sounds. Preferably, the system should allow encryption or other encoding of one or more of the selected components and should allow change of
- 10 parameters affecting the format of one or more of the components.

Summary of the Invention

- These needs are met by the invention, which provides a system for removing one or more selected segments (referred to collectively as pre-processing components, or PPCs) of a digital signal stream that represents
- 15 an assembly of information-bearing sounds (ISA), including but not limited to music and one or more human voices, to produce a remainder data file (referred to as a reduced data file, or ISDF), having one or more components, after decimation of the ISA by removal of the PPC(s). The
- 20 ISDF, as a first sequence, and the assembly of PPCs, as a second sequence are preferably processed differently and communicated using different communication channels. The ISDF is preferably encrypted or otherwise encoded, using an encryption key EK that may be chosen independently or may depend upon information contained in the PPC(s). A data supplement
- 25 DS, associated with the PPC(s) sequence, contains one or more of the following information items: location of at least one PPC within the original ISA; size of one or more of the PPCs; size of one or more components of the ISDF; separation distance within the ISA of two consecutive PPCs (if

two or more are removed); and at least a portion of the encryption key EK. The encrypted version of the ISDF, $E(\text{ISDF})$, is communicated over a first communication channel, and the PPC(s) and the associated data supplement DS are communicated over a second communication channel, which may be arranged as a secure communication channel. Optionally, the PPC(s) and associated data supplement channel may also be encrypted for communication. Optionally, more than one sequence of removed PPCs can be formed, each with an associated data supplement DS, and communicated separately from the remaining ISDF component(s).

10 The invention allows an assembly of information-bearing sounds ISA, such as music or the sound(s) of one or more human voices, to be disassembled into $N+1$ complementary sequences ($N+1$), where any collection of $N+1-k$ sequences ($1 \leq k \leq N$), including the ISDF, will not allow reconstruction of an assembly of sounds resembling the original ISA.

15 One useful application of this invention is the provision of a legally protected ISA (e.g., an ISA covered by copyright) as $N+1$ sequences, where any collection of N or fewer sequences cannot be used to reproduce the original ISA. The invention would, for example, allow distribution of a subset $N+1-k$ of these $N+1$ sequences to a prospective authorized listener at one time (e.g., for storage for possible future use) and distribution of the remaining k sequences ($1 \leq k \leq N$) at another time, when the listener is now authorized to listen to the entire ISA.

25 Another useful application of the invention is the provision or earlier distribution of a first sequence, representing the bulk or majority of the sounds needed to accurately reproduce the ISA, where the first sequence has certain critical data removed. The second sequence, containing the remainder of the ISA data needed to accurately reproduce the ISA, is distributed using another channel and/or at another, more convenient time.

Brief Description of the Drawings

Figure 1 is a schematic view of apparatus that creates an MP3 file.

Figures 2A-2C illustrate an original ISA, expressed as a digital sequence, and the results of disassembly of the ISA into an ISDF and a sequence of PPCs and of association of a DS with a PPC sequence.

Figure 3 is a schematic view of a digital file sampling composer and a digital file sampling synthesizer.

Figures 4, 5 and 6 are flow charts illustrating practice of embodiments of the invention.

Description of Best Modes of the Invention

MP3, which refers to Layer 3 of the MPEG1 standard, has been developed and adopted as a useful audio compression standard for music and other assemblies of information-bearing sounds (ISAs). MP3 is discussed in some detail in ISO/IEC 11172-3, an international standards document, incorporated by reference herein. A protocol for creation of an MP3 file is well known to those of ordinary skill in the art of sound compression. Many software programs, such as Audio Catalyst, offered by Xing Technology, which runs on a personal computer, implement creation of an MP3 file.

Figure 1 illustrates apparatus 11 that may be used to create an MP3 file 13 from an ISA 15. The ISA 15 is received by a digital file sampling composer (DFSC) 17. The DFSC 17 creates and issues a synthesizer information file (SIF) 19 and an item specific data file (ISDF) 21. For decoding, a DFS synthesizer 23 receives and uses the SIF 19 to provide suitable sequencing for the ISDF 21. The recovered MP3 file 13 is received and decoded by an MP3 decoder 25, which issues a pulse code modulation (PCM) waveform 27. The PCM waveform 27 can be played or otherwise

"displayed" through a digital-to-analog converter (DAC) 29, connected to a speaker 31.

Figures 2A-2C illustrate an ISA 15 as an ordered sequence of bits, nibbles, bytes or other information units, numbered $n = 1, 2, \dots, 27$, that are part of an ISA. The ISA (e.g., an MP3 source file) 15 can be any length. A first subset of these information units, namely "2", "5", "6", "7", "12", "17", "18", "26", "27", is removed as a sequence of pre-processing components (PPCs) and is stored in an SIF 19. The remaining data are stored in an ISDF for encryption. In Figure 2A, the ISA 15 is shown with a 32-bit header (or trailer, if desired), 27 bytes of data and an ID3 tag. The ISDF 21, shown in Figure 2B, has a file identification (FID) tag and a data field with a selected number of bytes of samples. The SIF 18, shown in Figure 2C, has an FID field, an ID3 tag, a 32-bit header field, a 2 byte file block (FB) field, a 2 byte song block (SB) field, a variable block size (BS) field, a 1-bit end-of-selection (EOS) flag and at least a portion of an encoding/encryption key (EK). The field block FB specifies the number of blocks of data for the ISDF 21. The song block SB specifies the number of blocks of data to be removed for the SIF 21, preferably using a file stripping algorithm. The block size field BS specifies the number of bits per block, which may be uniform or may be non-uniform. The EOS flag indicates that the coding process ended on data for the SIF 19 (EOS=1) or ended on data for the ISDF 21 (EOS=0).

Figure 3 illustrates a DFSC 17, which includes a first CPU 41, a first RAM 43, a first ROM 45, a first user interface 47, a removable storage unit 49, a data I/O module 51, and first and second communication channels, 53 and 55. The first interface 47 may include any or all of a keypad, keyboard, light pen or other data/command entry device, a mouse, and a display module, such as a monitor, LED or LCD device. The first and second

channels, 53 and 55, may be the same channel. Alternatively, the first and second channels may be different. For example, the second channel 55 may be a secure channel that offers at least a reasonable degree of protection against unauthorized reception of the signals on the second channel.

5 Figure 3 also illustrates a DFSS 23, which includes a second CPU 61, a second RAM 63, a second ROM 65, a second user interface 67, a data I/O module 69, a data synthesizer database 71, a removable storage device 73, and a DAC 75. The data synthesizer database 71 may include an ISDF database 71A and/or an SIF database 71B. The removable storage device 73
10 may include an ISDF database 73A and/or an SIF database 73B.

Digital samples that are part of the ISDF 21 and/or are part of the SIF 19 may be transferred from the DFS composes 17 to the DFS synthesizer 23 using the first communication channel 53 (for ISDF samples) and/or the second communication channel 55 (for SIF samples) and/or may be
15 recorded using the removable storage device 73 and subsequently transferred to the DFS synthesizer 23.

In a preferred embodiment, at least one of the first and second communication channels, 53 and 55, is the Internet. However, any other communication channel(s) can be used to communicate ISDF samples
20 and/or SIF samples, including wireless methods, such as FM subcarrier, CDPD, transmission using the vertical blanking interval of a television signal, and other similar wireless methods.

The ISDF database 71A and the SIF database 71B may include samples from any of several sample sources.

25 The DFS synthesizer 23 can operate in many different modes, including the following: (1) synthesize an MP3 file from an ISDF database 71A and from SIF samples streamed from the second communication channel 55; (2) synthesize an MP3 file from ISDF samples streamed from

the first communication channel 53 and from an SIF database 71B; (3) synthesize an MP3 file from an ISDF database 73A and from SIF samples streamed from the second communication channel 55; and (4) synthesize an MP3 file from an ISDF database 71A and from an SIF database 73B.

5 Figure 4 is a flow chart illustrating a procedure for practicing audio synthesis according to the invention. In step 81, an ISA including an ordered sequence of units containing digital symbols, is provided. In step 83, the PPCs within the ISA are designated and stripped out or removed from the remainder ISDF of the ISA. In step 85, a file identification number
10 FID is assigned to the PPCs and to the ISDF. In step 87, one or more parameters that characterizes the PPCs and/or the ISDF components is provided and is placed in a data supplement DS that is associated with the PPCs (preferable), to provide an augmented PPC sequence, PPC+DS, and/or with the ISDF. In step 89, an encoding key EK (e.g., an encryption
15 key) is provided, either independently or using one or more parameters provided by one or more components of the PPCs. Normally, the EK will have a fixed encoding procedure but optionally will have one or more parameters that are adjustable according to information supplied by the PPCs or the ISDF. For example, one or more PPCs may provide initial
20 values needed to begin the encoding process. In step 91, the ISDF (or an augmentation ISDF+DS) is encoded (e.g., encrypted), using the encoding key EK, to produce an encoded version E(ISDF). In step 93 (optional; usually not necessary), the augmented PPC sequence, PPC+DS, is also encoded to provide an encoded version E(PPC+DS).
25 In step 95, the encoded version E(ISDF) is communicated using a first communication channel, and the augmented PPC sequence, PPC+DS, is communicated using a second communication channel. The first and second communication channels may be the same, if desired. Alternatively,

the second communication channel may be a secure channel, to protect an non-encoded augmented PPC sequence, PPC+DS, from disclosure to unauthorized entities.

In step 97, the encoded version E(ISDF) and the augmented PPC
5 sequence, PPC+DS (or E(PPC+DS)), are received or otherwise provided,
and a decoding (e.g., decryption) process is begun. In step 99, the data
supplement DS within the augmented PPC sequence, PPC+DS, is
examined, the PPC and/or ISDF parameters are identified, and (optionally)
part or all of the encoding key EK is recovered. In step 101, the encoded
10 version E(ISDF) is decoded, to (re)produce the ISDF. In step 103, the PPC
components are repositioned among the ISDF components to recover the
original ISA. In step 105 (optional), the ISA is provided for an ISA
repository for playback, display, storage or further processing.

Optionally, the steps 97-103 may be varied by providing a first of the
15 two sequences, E(ISDF) or PPC+DS, in a first database that is available at
one or more locations to any potential user. However, possession of the first
sequence, or of the second sequence, along, does not allow the user to
reproduce the sounds of the original ISA. Each of the first sequence and the
second sequence is a decimated version of the original ISA; and the sounds,
20 if any, reproduced by the first sequence or by the second sequence alone
are, preferably, not intelligible. The second sequence is withheld until the
user has obtained proper authorization (e.g., a license) to reproduce the
sounds of the original ISA. The first sequence may, if desired, represent the
majority or bulk of the digital signals needed to reproduce the original ISA
25 so that the remainder (second sequence) requires far less bandwidth or
communication capacity for delivery than does the original ISA.

The encoding procedure may, for example, incorporate an encryption
process, such as cipher block chaining (CBC), described by Bruce Schneier,

Applied Cryptography, John Wiley & Sons, Second Edition, 1996, pp. 193-197. In one implementation of CBC, a cleartext block of a selected size is EXclusively ORed (XORed) or EXclusively NORed (XNORed) with a key block and with a preceding ciphertext block to produce a new ciphertext block. The resulting ciphertext block is XORed or XNORed with a next consecutive cleartext block and with the next consecutive key block, and so on until a final encrypted block is generated. The operations XOR and XNOR are each symmetric, commutative, associative and bilinear so that order is not important within the i th step. If P_i , C_i and K_i ($i = 1, 2, \dots$) represent cleartext block number i , ciphertext block number i and key block number i , respectively, a CBC procedure can be represented mathematically as

$$C(i+1) = P_i \text{ XNOR } C_i \text{ XNOR } K_i, \quad (1)$$

and the initial ciphertext block ($i=1$) can be specified by one or more of the PPCs. The choice XNOR, rather than XOR, is made here because of a useful "inversion" relation

$$A \text{ XNOR } A = I \text{ (identity)} \quad (2)$$

for any block A of binary symbols. With this approach, preferably, the size of a key block K_i is the same as the size of a cleartext block P_i and is the same as the size of a cipher text block C_i . This constraint can be relaxed somewhat.

When the encrypted message $E(\text{ISDF})$ is received, the process is reversed, beginning with an initial ciphertext block C_i' that is determined using information obtained from that data supplement component(s) received as part of the encrypted message $E(\text{ISDF})$:

$$P(i+1) = C(i+1)' \text{ XNOR } C_i' \text{ XNOR } P_i. \quad (3)$$

Each of Eqs. (1) and (3) illustrates a sub-encryption cycle (or sub-decryption cycle) for the encryption or decryption process, where an initial

ciphertext block is optionally provided by a key block K_i with $i = 1$. Each sub-encryption cycle, set forth as an example in Eq. (1), will have an independently specified key component K_i .

Figure 5 is a flow chart illustrating a file stripping algorithm that can be applied to an ISA using an embodiment of the invention. In step 111, a first sequence of units (to hold an ISDF) and a second sequence of units (an SIF to hold the PPCs) are created; each of unspecified length, and the same FID is assigned to each sequence. The assembled first and second sequences will resemble the sequences shown in Figures 1B and 1C. In step 113, a strip count index SC is set equal to the specified number SB of PPCs. In step 115, the first PPC, or the next PPC in the ordered sequence of PPCs, is moved from the initial sequence (Figure 1A) to that PPC's assigned place in the second sequence. A selected portion of this PPC (which may be the empty set for a particular PPC) is stored in a location, denoted as TK, for future use. The particular arrangement of bits or other information units stored in TK is referred to herein as the "content" of TK, written TK(c). A portion of this content TK(c) can also be used to determine one or more parameters for the encryption key EK.

In step 117, the strip count index SC is decremented by 1 ($SC = SC - 1$). In step 119, the system examines the last unit in the particular component of the second sequence (PPCs) and determines if this last unit is an end-of-file unit ($EOF = 0$). If the answer to the query in step 119 is "yes", the system sets an EOK flag equal to a selected value (e.g., $EOK = 1$), in step 121, and the procedure terminates at step 123.

If the answer to the query in step 119 is "no", the system determines if the strip count index satisfies $SC \leq 0$; in step 127. If the answer to the query in step 127 is "no", the system recycles to step 115 and the procedure continues. If the answer to the query in step 127 is "yes", the system

initializes the strip count index to $FB + TK(c1)$, in step 129, where $TK(c1)$ is a selected subset of the content $TK(c)$ held at the location TK . Use of a combination $FB + TK(c1)$, with $TK(c1)$ variable, allows the number of sub-cycles covered in the (following) steps 121 through 129 to be varied or

5 "dithered" within the procedure.

In step 131, the system encrypts the first block, or the next consecutive block, in the first sequence of units (ISDF). In step 133, the system decrements the (new) strip count index SC ($SC = SC - 1$). In step 135, the system determines if an EOF is present in this block. If the answer to the query in step 135 is "yes", the procedure terminates at step 137. If the

10 answer to the query in step 135 is "no", the system determines if the (new) strip count index satisfies $SC \geq 0$, in step 139. If the answer to the query in step 139 is "no", the system recycles to step 131 and the procedure continues. If the answer to the query in step 139 is "yes", the system recycles to step

15 113 and the procedure continues.

Figure 6 is a flow chart illustrating a file assembly procedure that can be used with an embodiment of the invention. In step 141, the system identifies the data supplement DS and reads the parameters FB , KB , $SISFD$, $SPPC$, EOK and EK . In step 143, the system initializes an assembly count index, $AC = SB$. In step 145, the system moves the first block, or the next

20 consecutive block, of the first sequence of units (PPC) to its proper location in the original sequence of units (specified by SB , FBS and KBS) and stores a selected portion of the PPC information (which may be the empty set) at a designated location TK . In step 147, the system decrements the assembly

25 count index ($AC = AC - 1$).

In step 149, the system examines the last unit in the particular component of the second sequence (PPCs) and determines (1) if this last unit is an end-of-file unit and (2) if $EOK = 1$. If the answers to the

compound query in step 149 are "yes" and "yes", the procedure terminates, at step 151. If the answer to one or both parts of the compound query in step 149 is "no", the system sets the EOK flag equal to another selected value (e.g., $EOK = 0$), in step 155. In step 157, the system determines if the
5 assembly count index satisfies $AC \geq 0$.

If the answer to the query in step 157 is "no", the system recycles to step 145 and the procedure continues. If the answer to the query in step 157 is "yes", the system resets an initial assembly count index, $AC = FB + TK(c1)$, in step 159, where $TK(c1)$ is a selected subset of the content $TK(c)$.
10 Again, use of a combination $FB + TK(c1)$, with $TK(c1)$ variable, allows the number of sub-cycles covered in the (following) steps 161 through 169 to be varied or "dithered" within the procedure.

In step 161, the system decrypts the next consecutive block of a reassembled original sequence. In step 163, the system decrements the
15 (new) assembly count index ($AC = AC - 1$). In step 165, the system examines the last unit in the particular component of the first sequence (ISDF) and determines (1) if this last unit is an end-of-file unit and (2) if $EOK = 0$. If the answers to this compound query in step 165 are "yes" and "yes", the system terminates the procedure, at step 167. If the answer to one or both parts of
20 the compound query in step 165 is "no", the system determines, at step 169, if the assembly count index AC satisfies $AC \geq 0$. If the answer to the query at step 169 is "no", the system recycles to step 161 and the procedure continues. If the answer to the query in step 169 is "yes", the system recycles to step 143 and the procedure continues.

25 In another embodiment, no PPCs are removed, and the entire file becomes an ISDF. No data supplement DS need be included, unless (part of) the encoding/encryption key EK is to be communicated with the encoded/encrypted version $E(ISDF)$ or as part of an SIF. Otherwise, the SIF

and the DS may be deleted in this embodiment. With reference to Figure 4, steps 87, 93, 99 and/or 103 are optionally deleted in this embodiment. The file stripping algorithm, shown in Figure 5, and the file assembly algorithm, shown in Figure 6, are not used in this embodiment; this may also be
5 implemented by formally setting $FB = SB = 0$ in Figures 5 and 6.

The disclosed procedure relies primarily upon several features to provide secure communication of an ISA, as two or more sequences, where no combination of less than all the sequences will produce an assembly of sounds that adequately resemble the original ISA. First, portions of the
10 message, the PPCs, are removed from the original ISA and are communicated separately, optionally using a secure channel. Second, the remainder of the ISA, the ISDF, is encrypted, using an encoding or encryption key that can vary in length and other characteristics from one block or component of the ISDF to another, as indicated in the discussion of
15 Figures 5 and 6. Third, information in one or more of the PPCs can be used to determine one or more parameters in portions of the encoding or encryption key EK. Fourth, an augmented PPC sequence PPC+DS can also be encoded and/or encrypted before communication thereof.

Among other things, an unauthorized (or unlicensed) recipient of the
20 encoded/encrypted version $E(ISDF)$ and/or of the augmented PPC sequence PPC+DS would need to be aware of (1) the encoding or encryption key used to process the encoded/encrypted version $E(ISDF)$ (and, optionally, used to encrypt the augmented PPC sequence PPC+DS); (2) the placement and meaning of ISDF, PPC and/or EK information contained in the data
25 supplement DS; (3) the use of the information in the data supplement DS to reposition the PPCs within a decoded or decrypted ISDF, and (4) possible variation of the encoding/encryption key from one ISDF component to the next, in order to fully decode or decrypt an intercepted ISDF representing

and ISA. The number of parameters and block-to-block variability incorporated in this system allows one to distribute or otherwise provide one or more, but less than all, of the sequences formed from the ISA, without making available any version that can be intelligibly played back.

- 5 The missing sequence(s) from the ISA can be distributed to licensed or otherwise authorized "listeners", by another channel and/or at another time.

What is claimed is:

1. A method of encoding or encrypting data, characterized by:
providing an assembly of information-bearing sounds (ISA);
5 removing one or more selected segments of the assembly, to produce
a specified data file;
providing an encoding/encryption key and encoding or encrypting the
specified data file; and
communicating the encoded or encrypted specified data file in a first
10 selected communication channel and communicating the removed segments
in a second selected communication channel.

2. The method of claim 1, further characterized by providing a data
supplement that indicates at least one of: location of at least one of said
15 removed segments within said ISA; size of at least one of said removed
segments within said ISA; number of segments removed; separation
distance between two consecutive removed segments within said ISA; and a
selected portion of said encoding/encryption key; and
communicating said data supplement in said second selected
20 communication channel.

3. The method of claim 1, further characterized by providing said
encoding/encryption key with at least one key parameter that uses
information from at least one of said removed segments.

25

4. The method of claim 1, further characterized by selecting said first
and second communication channels to be the same channel.

5. The method of claim 1, further characterized by providing said second channel as a secure communication channel.

6. The method of claim 1, further characterized by concatenating said removed segments and said data supplement as a concatenated data file.

7. The method of claim 6, further characterized by encrypting said specified data file using cipher block chaining of at least one block of said concatenated data file and at least one encrypted block from said specified data file.

8. The method of claim 7, further characterized by providing said at least one encoding/encryption parameter for said encoding/encryption key by providing a block of said concatenated data file as an initial block for said at least one encrypted block of said data.

9. The method of claim 1, further characterized by removing at least first and second segments from said data file, where the first segment and the second segment have equal length.

10. The method of claim 1, further characterized by removing at least first and second segments from said data file, where the first segment and the second segment have different lengths.

11. The method of claim 1, further characterized by combining said removed segments with said specified data file to form a combined data file and reproducing the combined data file as an assembly of sounds.

12. A method of decoding or decrypting data, characterized by:
providing an encoded or encrypted first data file;
providing a second data file and a data supplement that indicates at
least one of: an assigned location of at least one designated segment of the
5 second data file within a non-coded and non-encrypted version of the first
data file; size of at least one designated segment of the second data file
within the non-coded and non-encrypted first data file; number of selected
segments designated; separation distance of at least two consecutive
designated segments of the second data file within the non-coded and non-
10 encrypted first data file; and a selected portion of an encoding/encryption
key used to encode or encrypt the first data file; and

using the data supplement to decode or decrypt the encoded or
encrypted first data file and to position at least a first sequence and a second
sequence, drawn from the second data file, within the first data file.

15

13. The method of claim 12, further characterized by providing said
encoded or encrypted first data file on a first communication channel and
providing said concatenation of said second data file and said data
supplement on a second communication channel.

20

14. The method of claim 13, further characterized by selecting said
first and second communication channels to be the same channel.

15. The method of claim 13, further characterized by providing said
25 second channel as a secure communication channel.

16. The method of claim 19; further characterized by determining at least one parameter of said encoding/encryption key using information in said second data file.

5 17. The method of claim 12, further characterized by providing said encoded or encrypted first data file using cipher block chaining of at least one block of said concatenation of said second data file and said data supplement and at least one encoded or encrypted block from said first data file.

10 18. The method of claim 17, further characterized by providing at least one encoding/encryption key parameter for said encoding/encryption key by providing at least one of said first sequence and said second sequence as an initial block for said at least one encoded/encrypted block of
15 said data.

19. The method of claim 12, further characterized by providing said second data file and said data supplement as a concatenated data file.

20 20. The method of claim 12, further characterized by combining said removed segments with said specified data file to form a combined data file and reproducing the combined data file as an assembly of sounds.

21. A method of communicating data, characterized by:
25 providing an assembly of information-bearing sounds as a digital file of data;
removing one or more selected segments from the data file, to produce a specified data file having at least a first block and a second block;

providing an encoding/encryption key having at least a first key portion and a second key portion;

providing a data supplement that indicates at least one of: location of at least one of the removed segments within the data file; size of at least one of the removed segments within the data file; number of segments removed;

5 separation distance between two consecutive removed segments within the data file; and at least a portion of the encoding/encryption key;

encoding or encrypting the first block and the second block of the specified data file, using the first portion and the second portion, respectively, of the encoding/encryption key; and

10

communicating the encoded or encrypted specified data file in a first selected communication channel and communicating the removed segments and the data supplement in a second selected communication channel.

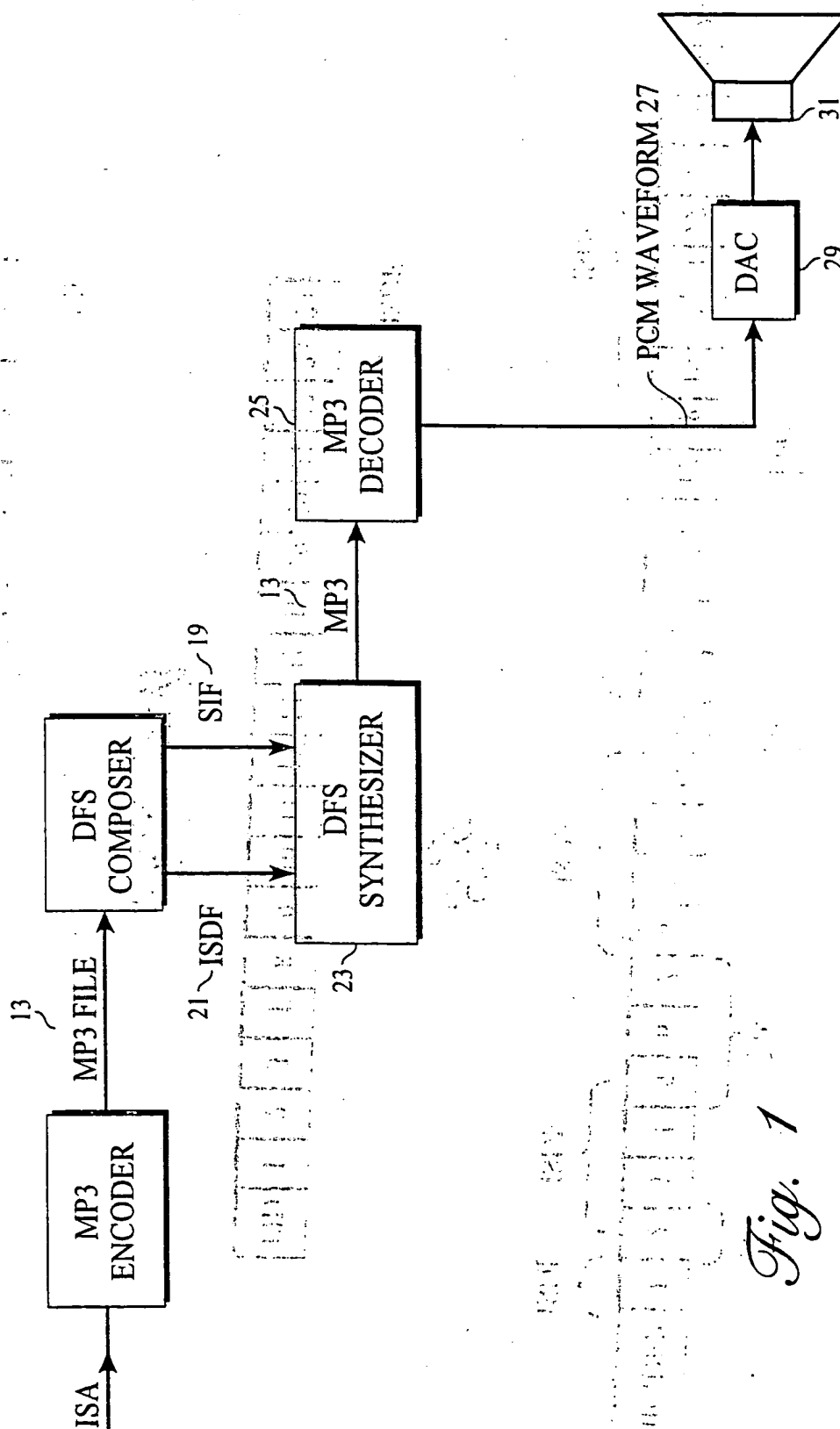


Fig. 1

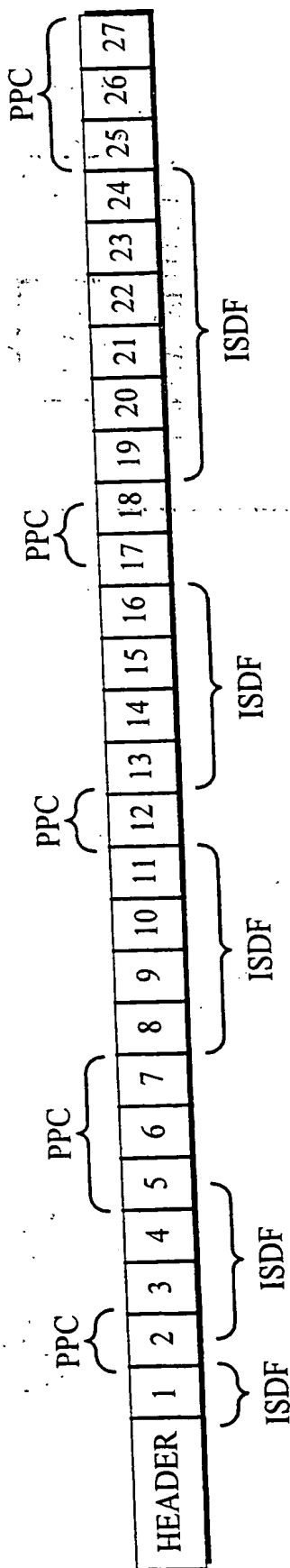


Fig. 2A

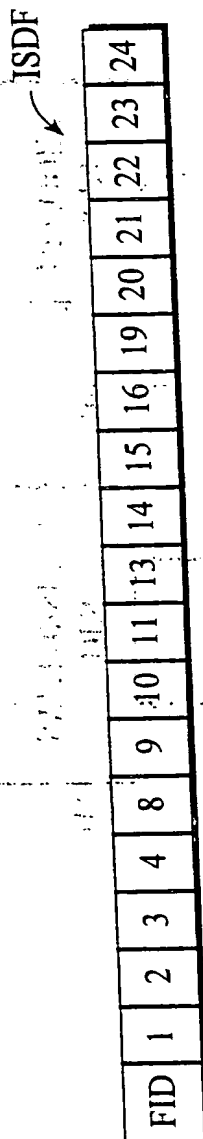


Fig. 2B

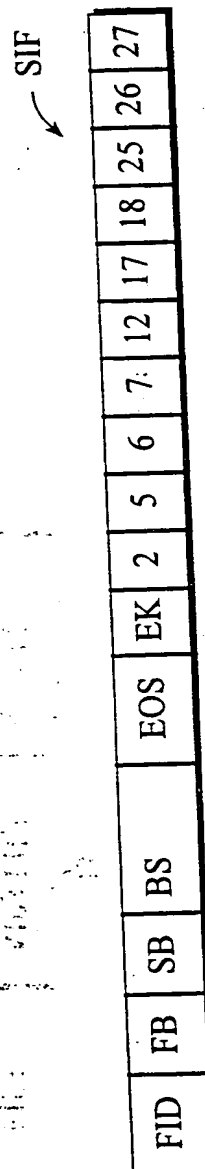


Fig. 2C

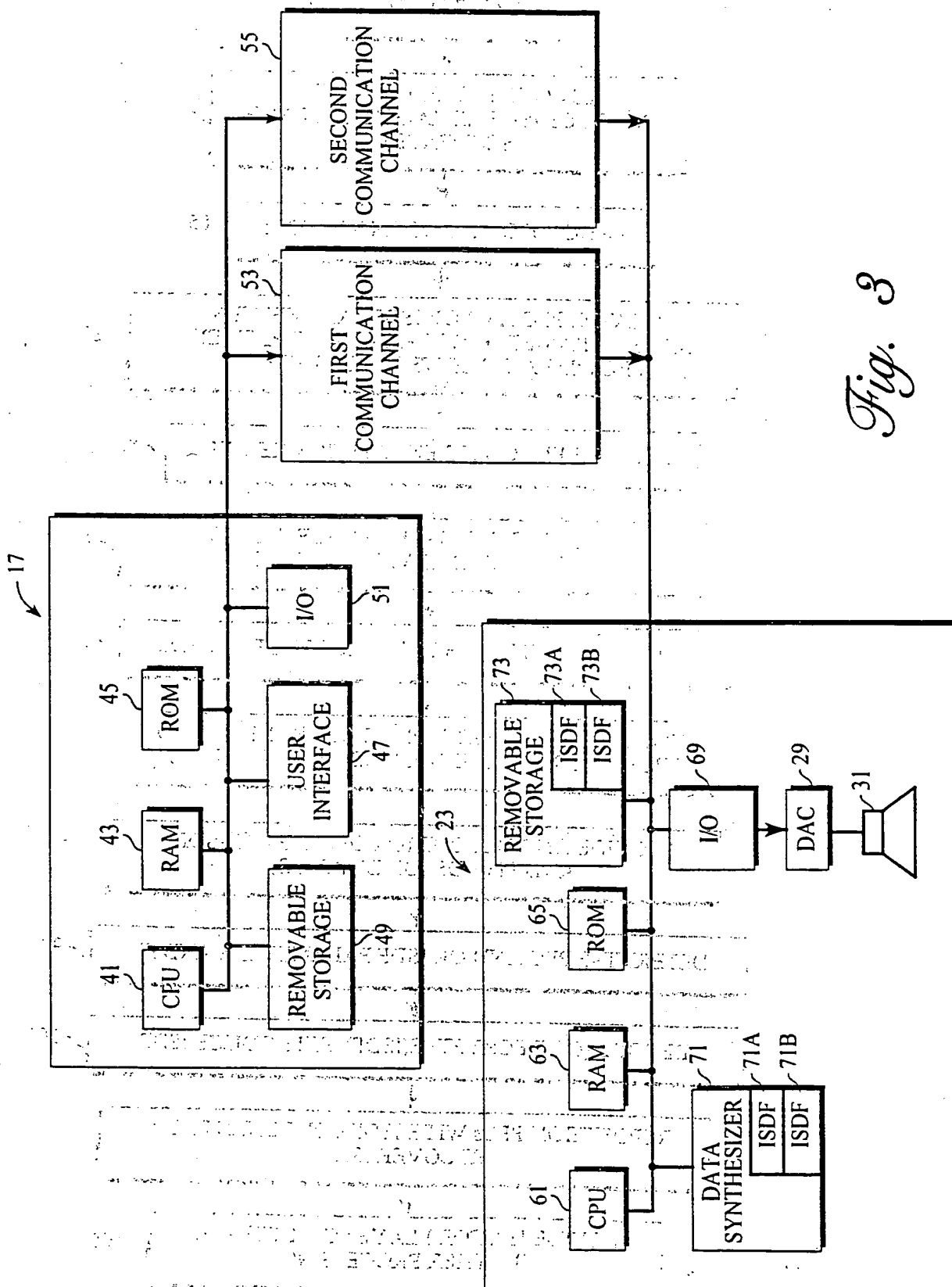


Fig. 3

4/6

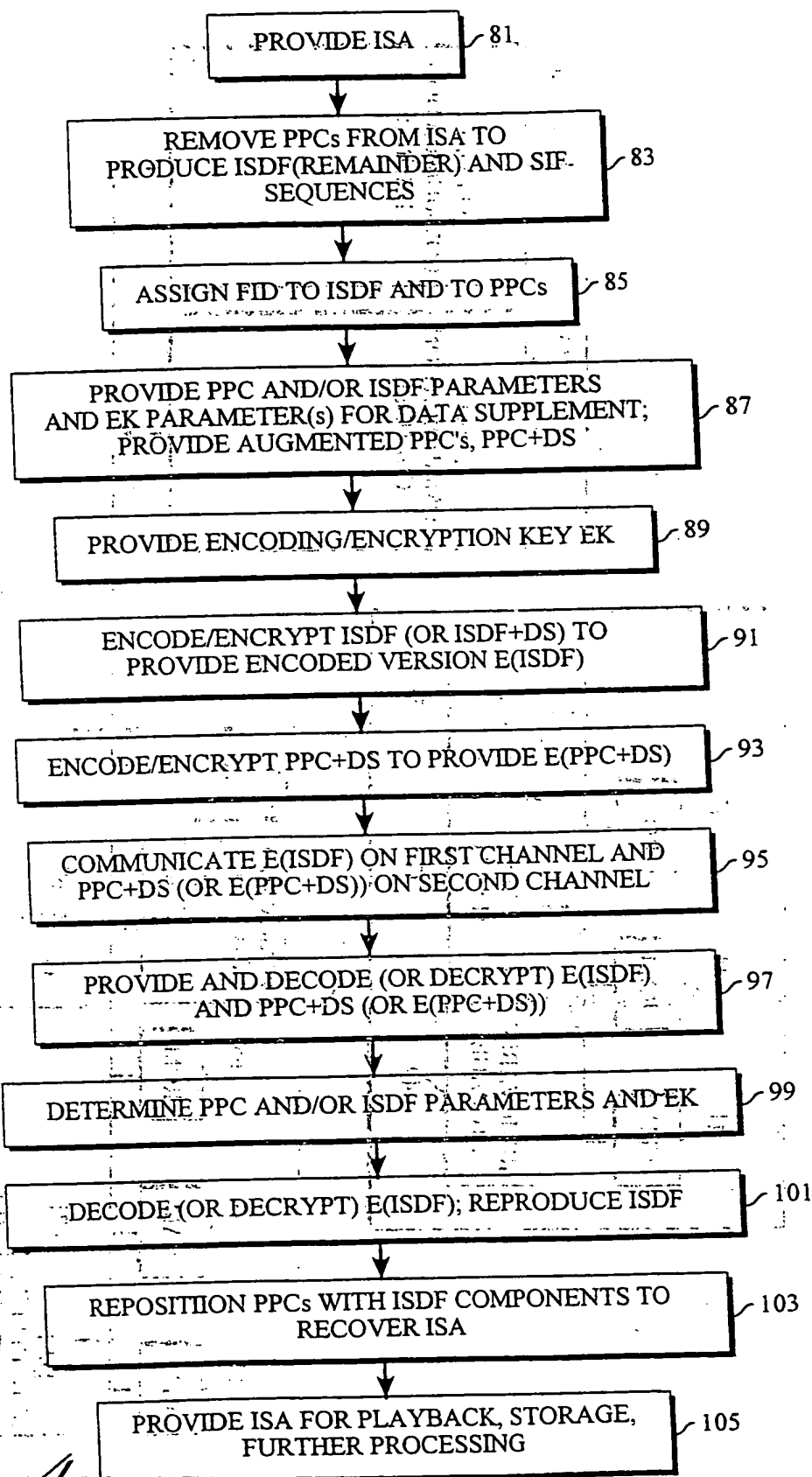


Fig. 4

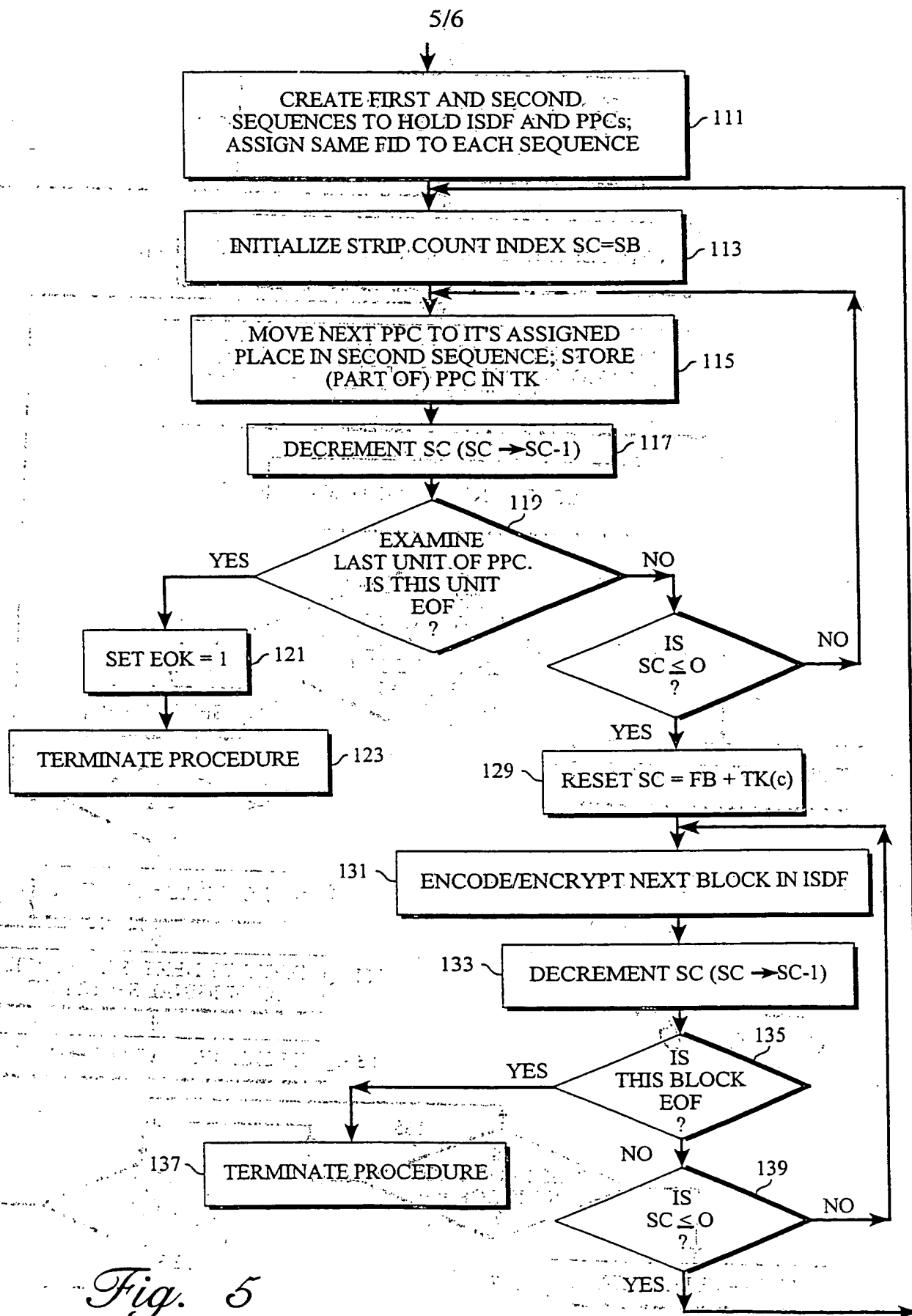
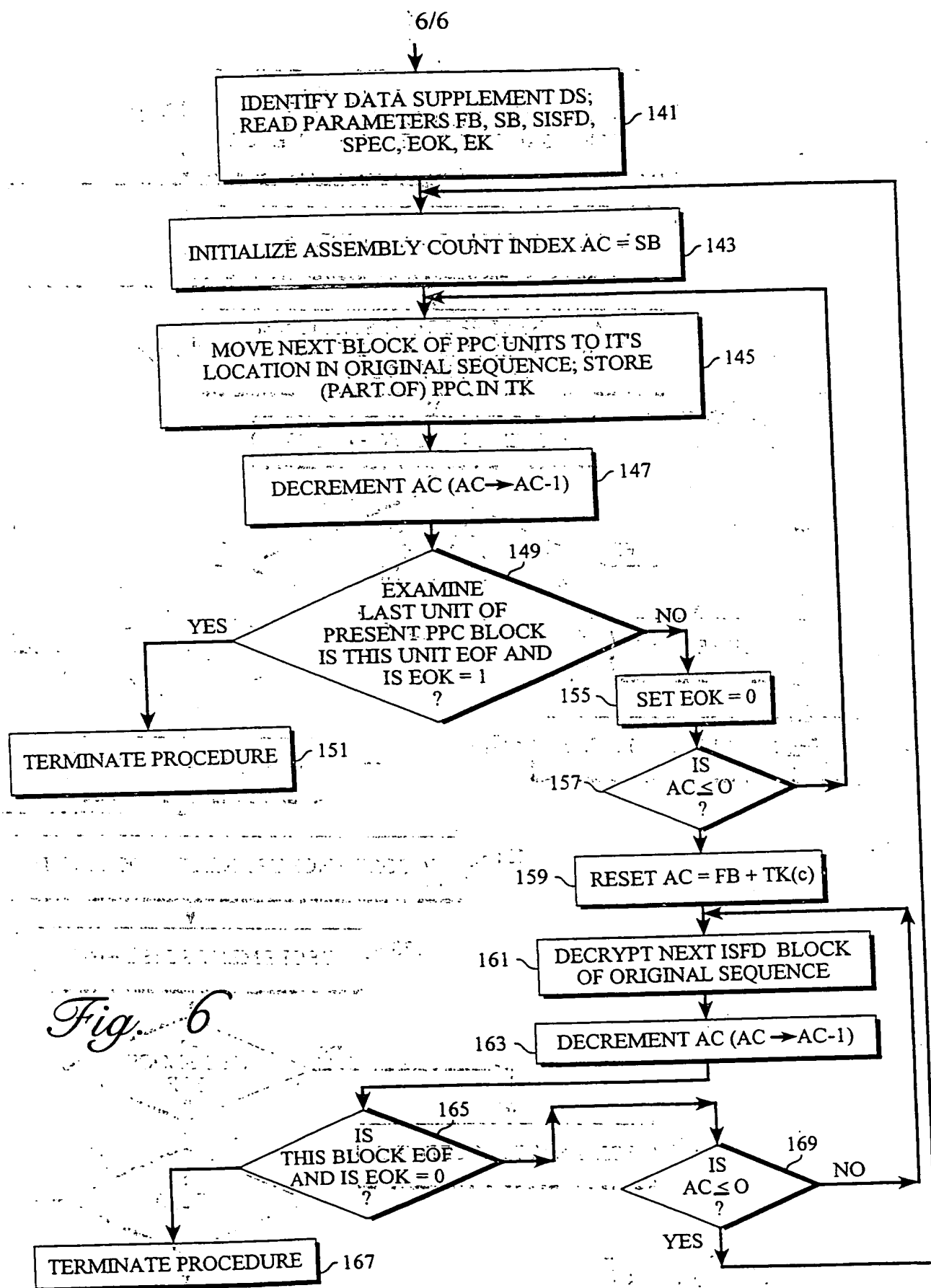


Fig. 5



INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/04012

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G10H1/00 H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G10H H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 636 276 A (BRUGGER ROLF) 3 June 1997 (1997-06-03) column 4, line 41 -column 5, line 59; figures 1-3	1-4, 12-14,21
A	EP 0 843 449 A (SUNHAWK CORP INC) 20 May 1998 (1998-05-20) column 5, line 53 -column 7, line 58; figure 1	1,12,21
A	US 5 773 741 A (MILLS BRENT R ET AL) 30 June 1998 (1998-06-30) column 4, line 1 -column 6, line 31; figure 1	1,12,21
A	GB 2 222 057 A (CARRIDICE LTD) 21 February 1990 (1990-02-21) page 1; figure 1	1,5,11, 12,15,21
	-/-	



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

5 July 2000

Date of mailing of the international search report

12/07/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Pulluard, R

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/04012

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>YAMAMOTO H: "ON SECRET SHARING COMMUNICATION SYSTEMS WITH TWO OR THREE CHANNELS"</p> <p>IEEE TRANSACTIONS ON INFORMATION THEORY, US, IEEE INC. NEW YORK, vol. IT-32, no. 3, 1 May 1986 (1986-05-01), pages 387-393, XP000764636</p> <p>ISSN: 0018-9448</p> <p>page 387, left-hand column; figure 2</p>	<p>1, 11, 12, 15, 21</p>

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/US 00/04012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5636276 A	03-06-1997	DE 4413451 A	14-12-1995
		AT 169762 T	15-08-1998
		DE 59503112 D	17-09-1998
		EP 0678851 A	25-10-1995
		ES 2119344 T	01-10-1998
		GR 3027730 T	30-11-1998
EP 0843449 A	20-05-1998	US 5889860 A	30-03-1999
		CA 2220457 A	08-05-1998
		JP 10301904 A	13-11-1998
US 5773741 A	30-06-1998	NONE	
GB 2222057 A	21-02-1990	NONE	